

FILED

UNITED STATES DISTRICT COURT

for the
Western District of Texas

September 30, 2020

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXASBY: klw
DEPUTYIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INFORMATION ASSOCIATED WITH FACEBOOK USER ID
https://www.facebook.com/profile.php?id=100008210433667 THAT IS
STORED AT PREMISES CONTROLLED BY FACEBOOK INC.

Case No. 1:20-mj-841 SH

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A, Section I.located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment A, Sections II and III.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
26 U.S.C. 5861(d)Offense Description
Possession of an unregistered NFA firearm/destructive device.

The application is based on these facts:

See attached Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Rey Alatorre, Jr., ATF Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 09/30/2020

Judge's signature

City and state: Austin, Texas

Susan Hightower, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
FACEBOOK USER ID

<https://www.facebook.com/profile.php?id=100008210433667>

THAT IS STORED AT
PREMISES CONTROLLED BY FACEBOOK
INC.

Case No. 1:20-mj-841 SH

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
INSTAGRAM USER ID

<https://www.instagram.com/cyrcalcs/>

THAT IS STORED AT
PREMISES CONTROLLED BY FACEBOOK
INC.

Case No. 1:20-mj-842 SH

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
TWITTER USER ID

<https://twitter.com/clartigue17?lang=en>

THAT IS STORED AT
PREMISES CONTROLLED BY TWITTER
INC.

Case No. 1:20-mj-843 SH

IN THE MATTER OF THE SEARCH OF
INFORMATION AND RECORDS ASSOCIATED WITH
Clartigue10@gmail.com THAT IS STORED AT
PREMISES CONTROLLED BY GOOGLE

Case No. 1:20-mj-844 SH

IN THE MATTER OF THE SEARCH OF
INFORMATION AND RECORDS
ASSOCIATED WITH ALL APPLE ACCOUNTS
ASSOCIATED WITH THE EMAIL ADDRESS
Clartigue10@gmail.com; AND/OR SUBSCRIBER
CYRIL LARTIGUE; AND/OR ASSOCIATED WITH
TELEPHONE NUMBER: (512)586-3046, THAT
IS STORED AT PREMISES CONTROLLED BY
APPLE INC.

Case No. 1:20-mj-845 SH

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS

I, Reynaldo Alatorre Jr., a Special Agent with the Bureau of Alcohol, Tobacco, Firearms
and Explosives, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for search warrants for certain social media, storage and email accounts described further in Section I of Attachments A, B, C, D and E (the “**Target Accounts**”), for certain things particularly described in Sections II & III of Attachments A, B, C, D, and E.

2. This affidavit is made in support of an application for search warrants under Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require the service providers to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the **Target Accounts**.

3. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and have been so employed since July 2001. Prior to my employment with the ATF, I was employed as a Border Patrol Agent for approximately four years. I am a graduate of the Federal Law Enforcement Training Center and the ATF National Academy. As a result of my training and experience, as an ATF Special Agent, I am familiar with firearms and with Federal Firearms Laws, including Title 26 offenses concerning destructive devices. I have also discussed this investigation with other ATF Special Agents with specialized experience in Destructive Devices (incendiary device(s)) and Destructive Device investigations.

4. As a result of my training and experience relating to these statutes, and the experience of other senior Special Agents and investigators, I believe that there is probable cause that evidence of the following offense will be found in the social media, storage and email accounts, listed in Attachments A, B, C, D and E:

Tile 26 United States Code 5861(d), It shall be unlawful for any person to receive or possess a firearm (destructive device) which is not registered to him in the National Firearms Registration and Transfer Record.

5. Your Affiant is aware that a destructive device is defined as follows:

Title 26 United States Code 5845(f)(3): The term destructive device means any combination of parts either designed or intended for use in converting any device into a destructive device as defined in this statute from which a destructive device may be readily assembled.

6. Based on my knowledge, training, and experience, I know persons engaged in criminal conduct typically use computers, cell phones and electronic devices to conduct research on the materials needed/procedures of manufacturing a destructive device and will typically maintain electronic evidence of such research.

7. Based on my knowledge, training, and experience, I know persons engaged in criminal conduct commonly use cell phones, electronic mail (e-mail), instant messaging (IM), or peer-to-peer file-sharing (P2P) to perpetuate their criminal conduct, particularly as a prevalent communication tool among groups engaging in illegal activity. Cell phones, electronic mail (e-mail), instant messaging (IM), and peer-to-peer file-sharing (P2P) frequently contain evidence of those communications and that even if they are deleted by the user they can often be recovered by a competent forensic examiner. Evidence of these cell phone, electronic mail (e-mail), instant messaging (IM), or peer-to-peer file-sharing (P2P) communications may be used to aid in the identification of additional co-conspirators, and to identify utilization or travel in interstate or foreign commerce to facilitate their criminal conduct, or manage, facilitate, distribute, or dispose of proceeds from their criminal conduct.

8. Based on my knowledge, training, and experience, I know that persons engaged in criminal conduct typically use computers, cell phones and electronic devices prior to and during the commission of their criminal conduct to communicate with co-conspirators, access electronic information for real time intelligence of their target locations, utilize applications and other

electronic information for addresses, maps, directions, and to avoid the detection by law enforcement.

9. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and law enforcement officers in this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

JURISDICTION

10. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

FACEBOOK AND RELATED SERVICES

11. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

12. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user’s full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

13. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

14. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

15. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user

and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

16. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

17. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

18. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

19. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

20. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

21. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

22. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

23. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

24. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

25. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may

communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

26. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location

in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

27. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INSTAGRAM AND RELATED SERVICES

28. Instagram owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.instagram.com>. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application (“app”) created by the company that allows users to access the service through a mobile device.

29. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various “tags” that can be used to search for the photo (e.g., a user made add the tag #vw so that people interested in Volkswagen vehicles can search for and

find the photo); location information; and other information. A user can also apply a variety of “filters” or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also “like” photos.

30. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by Instagram.

31. Instagram asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user’s full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram collects and maintains this information.

32. Instagram allows users to have “friends,” which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Instagram collects and maintains this information.

33. Instagram also allows users to “follow” another user, which means that they receive updates about posts made by the other user. Users may also “unfollow” users, that is, stop following them or block the, which prevents the blocked user from following that user.

34. Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Instagram collects and maintains user content that users post to Instagram or share through Instagram.

35. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user's feed, search history, or profile.

36. Users on Instagram may also search Instagram for other users or particular types of photos or other content.

37. For each user, Instagram also collects and retains information, called "log file" information, every time a user requests access to Instagram, whether through a web page or through an app. Among the log file information that Instagram's servers automatically record is the particular web requests, any Internet Protocol ("IP") address associated with the request, type of browser used, any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.

38. Instagram also collects and maintains "cookies," which are small text files containing a string of numbers that are placed on a user's computer or mobile device and that allows Instagram to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user's interests.

39. Instagram also collects information on the particular devices used to access Instagram. In particular, Instagram may record "device identifiers," which includes data files and other information that may identify the particular electronic device that was used to access Instagram.

40. Instagram also collects other data associated with user content. For example, Instagram collects any “hashtags” associated with user content (i.e., keywords used), “geotags” that mark the location of a photo and which may include latitude and longitude information, comments on photos, and other information.

41. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.

42. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user’s account activity, IP log, stored electronic communications, and other data retained by Instagram, can indicate who has used or controlled the Instagram account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was accessed or used. For example, as described herein, Instagram logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under

investigation. Additionally, Instagram builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Instagram “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner’s state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

43. Based on the information above, the computers of Instagram are likely to contain all the material described above with respect to the SUBJECT ACCOUNT, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

TWITTER AND RELATED SERVICES

44. Twitter owns and operates a free-access social-networking website of the same that can be accessed at <http://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to create and read 280-character messages called “Tweets,” and to restrict their “Tweets” to individuals whom they approve. These features are described in more detail below.

45. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

46. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, email address, physical address (including city, state, and zip code), dates of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the IP address at the time of sign-up. Twitter keeps IP logs for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile. This type of information can help to identify which computers or other devices were used to access a given Twitter account.

47. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" of 160 characters or fewer to their profile pages.

48. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 280-characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also "favorite", "retweet", or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the "@" sign, Twitter designates that Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have "favorited" or "retweeted" the user's

own Tweets, as well as a list of all Tweets that include the user's username (i.e., a list of all "mentions" and "replies" for that username).

49. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services. Twitter users can also opt to include location data in their Tweets, which will reveal the users' locations at the time they post each Tweet. This "Tweet With Location" function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data. Additionally, when Twitter users want to post a Tweet that includes a link to a website, they can use Twitter's link service, which converts the longer website link into a shortened link that begins with <http://t.co>. This link service measures how many times a link has been clicked.

50. A Twitter user can "follow" other Twitter users, which means subscribing to those users' Tweets and site updates. Each user profile page includes a list of the people who are following that user (i.e., the user's "followers" list) and a list of people whom that user follows (i.e., the user's "following" list). Twitter users can "unfollow" users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into "lists" that display on the right side of the user's home page on Twitter. Twitter also provides users with a list of "Who to Follow", which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

51. In addition to posting Tweets, a Twitter user can send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the

recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored in Twitter's database.

52. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user's mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent to the user's phone. Twitter also includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches. Twitter users can also connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

53. Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the providers or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

54. Thus, the computers of Twitter are likely to contain all the material described above. As is the case with Facebook, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation. A Twitter user's account information, IP log, stored electronic

communications, and other data retained by Twitter can indicate who has used or controlled the Twitter account and how and when it was accessed or used. Additionally, by reviewing Twitter's IP logs for a particular account, investigators can determine the physical location associated with the logged IP addresses, and thereby, learn the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to "tweeted" communications. This geographic and timeline information may tend to either inculcate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner's state of mind as it relates to the offense under investigation. For example, information on the Twitter account may include the owner's motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

GMAIL AND RELATED SERVICES

55. Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email account identified in Attachment E, Section I. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic information, which is significant to identifying those using and/or accessing the account.

56. A Google subscriber can store files with the provider in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails),

and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

57. I know from my training and experience that email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Such information may constitute evidence of the crimes under investigation because it can be used to identify the account's user or users. Even if subscribers insert false information to conceal their identity, such information often provides clues to their identity, location or illicit activities.

58. I know from my training and experience that email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of serviced, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of IP addresses used to register the account and associated with particular logins to the account. As previously stated, IP addresses can help to identify which computers or other devices were used to access the email account.

59. Email accounts will often communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from the users. Email providers typically retain records about such communications, including

records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

60. As previously stated, information stored in connection with an electronic account, such as an email account, provides crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, including identifying individuals using or accessing the account, their geographic location (based in IP addresses), and their state of mind as it relates to the offenses under investigation (to include motive, intent, and/or consciousness of guilt). Thus, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email from Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information.

APPLE INC. AND RELATED SERVICES

61. Based upon my training, experience, and from what I have been told by other law enforcement officers and resources, I know the following regarding "cloud storage" and the use of Apple's iCloud storage by users of iPhone, iPads, and other Apple products:

62. Internet companies have been creating platforms commonly referred to as "the Cloud." Simply put, "the Cloud" is third-party data storage space that a user can use to store and access files anytime, anywhere, with an Internet connection.

63. Apple has created a multitude of software and online services for computer users. One of those is the "iCloud" service. iCloud is part of Apple's range of online services. iCloud is a data storage service that allows customers to store data and files on servers belonging to and

maintained by Apple. iCloud can be used to automatically backup and store data on a customer's device that uses the Apple operating system (iOS). iCloud allows customers to upload and access the latest versions of their data, like photographs, documents, apps, notes, contacts, etc., on whatever device they are using. iCloud also allows customers to easily share photographs, calendars, locations, and more with friends and family.

64. Customers can access their iCloud account from a web browser, computer, iPhone, iPad, or other Apple iOS device. Customers access their iCloud through their Apple ID, which is a unique identifier used by Apple based on the customer's email address as registered by the customer. During registration, Apple may collect a variety of information, to include name, mailing address, phone number, email address, contact preferences, and credit card information. By using the Apple ID to access iCloud, a customer controls access to his/her files, allowing files to be kept private or shared with others, including contacts. Apple provides 5GB of free iCloud storage space to customers, which can be used to store email, documents, music files, photographs, videos, contact lists, account information settings, and iOS device backups (such as iPhone and iPads). If needed, customers can purchase additional iCloud storage space.

65. According to the iCloud Terms and Conditions on Apple's website, iCloud "creates automatic backups for iOS devices periodically, when the device is screen locked, connected to a power source, and connected to the Internet via a Wi-Fi network. iCloud will store a customer's last three backups; however, if a device has not backed up to iCloud for a period of 180 days, Apple reserves the right to delete the backups associated with that device. Backup is limited to device settings, device characteristics, photos and videos, documents, messages (iMessage, SMS, and MMS), ringtones, app data (including Health app data), location settings (such as location-based reminders that you have set up), and Home screen and app organization. Content purchased

from the iTunes Store, App Store, or iBookstore is not backed up, but may be eligible for download from those services, subject to account requirements, availability, and the applicable terms and conditions. Media synced from your computer is not backed up. If you enable iCloud Photo Library, your Photo Library will be backed up separately from the automatic iCloud backup. Your iCloud email, contacts, calendars, bookmarks, and documents are stored in, and can be accessed via iCloud on your devices and computers.”

66. With the ease, popularity, and convenience of backing up iOS devices to the iCloud and the free 5GB of storage provided by Apple, more and more Apple customers are utilizing iCloud to backup up their devices today instead of connecting their device to a computer and having to manually backup the device using iTunes.

67. iTunes is another service offered by Apple. iTunes is a free software application which customers use to organize and play digital music and video on their computers. It's also a store that provides content for customers to download for their computers and iOS devices. This content includes music, movies, TV shows, Podcasts, and apps purchased via the App store on a customer's iOS device. When a customer opens an iTunes account, basic subscriber information such as name, physical address, email address, and telephone number can be provided. Additionally, information regarding iTunes purchase/download transactions and connections, update/re-download connections, and iTunes Match connections may also be available from Apple.

PROBABLE CAUSE

68. Affiant's investigation began on May 31, 2020, when your Affiant received information concerning allegations of Federal Firearm Law violations by Cyril Laurence LARTIGUE.

69. On May 30, 2020, at 11:00 a.m., a Facebook posting belonging to “Cyril Laurence LARTIGUE” posted the following comment:

“Second amendment advocates, now’s REALLY your time, show up and show out. Cops are the ones in many cases being violent first or infiltrating protests to kick off violence or property damage to “justify” use of force on civilian protesters, and the head of state has said he would send in military forces to fire on civilians to enforce what they consider to be “order”. Isn’t this shit what we’re supposed to have our own guns for?”

This posting was no longer available when queried by your Affiant; a screenshot of this posting can be found in Austin Police Department Offense Report 2020-1511608.

70. On May 30, 2020, at approximately 10:40 p.m., during a public protest located directly adjacent to Austin Police Headquarters and the Austin Municipal Court Building, located at 715 E. 8th Street, Austin, TX, Cyril LARTIGUE was observed by Austin Police Department HALO (High Activity Location Observation) camera operators squatting down behind a porta-potty in the parking lot directly adjacent to the Austin Municipal Court entrance.

71. LARTIGUE was observed wearing a blue/white plaid long-sleeve shirt, yellow hardhat helmet, beige/tan pants, brown work boots, mask, and gloves.

72. LARTIGUE opened a glass bottle, emptying out the contents of the bottle onto the ground without taking a drink, and then removed a small piece of cloth material from his backpack and placed this cloth into the opening of the glass bottle.

73. LARTIGUE then removed the cloth material from the bottle and obtained a rectangular container from his backpack and began to pour/squirt the contents of the rectangular container into the opening of the glass bottle. After pouring the contents into the glass bottle, LARTIGUE used the same contents to saturate the cloth material he had previously placed into the mouth of the glass bottle. The rectangular container was later determined to be a bottle of lighter fluid.

74. LARTIGUE was then interrupted by the oncoming presence of APD Officers heading in his direction.

75. LARTIGUE fled the area, leaving the above-mentioned materials behind.

76. A few minutes later, at approximately 2251 hours and after the APD Officers left the area, LARTIGUE returned to the same parking lot to retrieve the destructive device he had begun manufacturing.

77. LARTIGUE walked a short distance towards the south IH-35 frontage road where he placed his backpack onto a grassy area and placed the destructive device into the backpack.

78. LARTIGUE was then observed walking toward the front entrance of the Austin Police Department Headquarters, located at 715 E. 8th Street, Austin, Texas 78701 (with the destructive device still in his backpack and on his person). At this time, APD Officers positioned atop the western portion of the IH-35 Interstate overpass began actively illuminating LARTIGUE. Based on reviewed radio communications, these officers were aware of the situation regarding the destructive device.

79. LARTIGUE, now being observed by Austin Police Department HALO cameras and AIR 1, then changed direction to head east under IH-35. On the AIR 1 video, LARTIGUE can be seen using what appears to be a smartphone like an iPhone. LARTIGUE was then observed entering one of the porta-potties located near the east frontage of IH-35.

80. APD Officers converged on LARTIGUE's last known location and he was detained without incident. LARTIGUE's backpack was found within the porta-potty. LARTIGUE was found to have changed clothes. Within his backpack, officers located the following items of interest: a yellow safety hard-hat, a Zippo-type lighter with the name "Cyril" engraved on it, a bottled labeled "Zippo Lighter Fluid," a blue/white/grey checkered/plaid long-

sleeve shirt, and several small sections of rags/T-shirt(s)/light fabric/clothing material. The original bottle shown in the video was not found. Information provided to your Affiant in June 26, 2020, revealed that a search of LARTIGUE'S backpack, incident to arrest, did contain two (2) beer bottles (one empty and one full bottled sealed). These bottles were subsequently disposed of as perishables are not accepted as property by the Travis County Jail.

81. LARTIGUE was arrested and charged with state offenses.

82. As a result of this arrest, in addition to the items mentioned about, law enforcement also seized one (1) black Apple iPhone 11.

83. On June 7, 2020, your Affiant received from Austin Fire Department Lieutenant Paul De Maio the preliminary results obtained from the Texas Department of Public Safety Laboratory for the liquid found in LARTIGUE's possession. This liquid was found to be positive for a light petroleum distillate.

84. On June 7, 2020, your Affiant consulted with ATF Explosives Enforcement Officer Alex Guerrero who was advised of the items found in LARTIGUE's possession, to wit: Zippo-type lighter, Zippo Lighter Fluid, and small sections of rags. Based on these items and the above video, ATF Explosives Enforcement Officer Guerrero concluded these items meet the definition of a destructive device as it relates to Title 26 USC 5845(f)(3).

85. Your Affiant knows through his training and experience that per the National Firearms Act of 1934, destructive devices are required to be registered with the National Firearms Registration and Transfer Record.

86. On June 8, 2020, your Affiant received the results of a National Firearms Registration and Transfer Record query re: LARTIGUE. Results revealed that LARTIGUE does not have any items registered to him.

87. On June 8, 2020, LARTIGUE was arrested on a federal arrest warrant issued by United States Magistrate Judge Andrew W. Austin, reference Criminal Complaint 1:20-MJ-501-AWA. LARTIGUE was later indicted by a federal grand jury for Possession of an Unregistered Destructive Device in violation of 26 U.S.C. § 5861(d), Case No. 20-CR-156-RP.

88. On June 8, 2020, LARTIGUE was transported to the ATF Austin Field Office where he was interviewed by your affiant and ATF Special Agent Robert Noble. LARTIGUE was advised, and agreed to waive, his Constitutional Rights.

89. LARTIGUE claimed to have attended the rally/protest by himself and he denied any membership into any organization.

90. LARTIGUE stated he first walked by the State Capital, but was advised the by other bystanders that the majority of the demonstrators had walked down towards 7th Street and IH-35 (in the vicinity of the Austin Police Department Headquarters). LARTIGUE admitted to picking up a traffic cone during his walk towards the protest. He stated he had seen video footage of Hong Kong protesters using traffic cones to extinguish tear gas canisters.

91. LARTIGUE admitted he was wearing a hard hat to protect him from any rubber bullets (fired by law enforcement), and he was wearing work-gloves in the event he came into contact with any tear gas containers so that he could “return” the tear gas to law enforcement.

92. LARTIGUE admitting to having a change of clothes in the event he was exposed to tear gas. He also admitted to having a spray bottle mixed with baking soda/water to alleviate any pain/burn relief caused by tear gas.

93. LARTIGUE stated the reason he attended the protest was because it was the closest protest to him and he believed in the cause. He had seen video after video of police-violence. He

additionally referenced speaking out against police brutality and the nature/mentality of policing in America.

94. LARTIGUE admitted that he, himself, had never been a victim of police brutality.

95. LARTIGUE admitted to the presence of the aforementioned items in his backpack (lighter, lighter fluid, cloth pieces).

96. LARTIGUE did recall having a beer bottle before being arrested, but he could not recall what happened to the bottle.

97. LARTIGUE was then shown some still images taken from the HALO video of him manufacturing/possessing the destructive device.

98. LARTIGUE admitted that after leaving the device due to the oncoming presence of Austin Police Department Officers, he went back to retrieve the items (destructive device) he had left behind. He wanted to retrieve any items that could be linked back to him.

99. LARTIGUE stated his only previous experience with Molotov cocktails was in video games. He stated if anyone saw the video, the viewer would clearly see his inexperience on how "those things" (Molotov cocktail) worked.

100. In my training and experience, and that of other experienced ATF Agents with expertise in Destructive Device making, I know and have learned that Destructive Device manufacturers often research methods of constructing Destructive Devices using the internet and other electronic devices.

101. A review of APD HALO videos adjacent to the demonstration scene revealed LARTIGUE walking eastbound on 7th Street and San Jacinto Blvd. at approximately 2200hrs. From this first observance until his ultimate arrest, by APD, LARTIGUE can be seen sporadically coming into camera view. On several of these occasions LARTIGUE is observed conversing with

unknown individuals, accessing his cellular phone, and using his cellular phone to video the events around him.

102. An open-source query of Facebook revealed a Facebook profile under the name “Cyril LARTIGUE” containing a photo that is consistent with the individual interviewed by your Affiant. In this profile: <https://www.facebook.com/profile.php?id=100008210433667>, under the name Cyril LARTIGUE, in the “About” tab, LARTIGUE identifies he is from Cedar Park, Texas. Your Affiant is aware that LARTIGUE was living in Cedar Park, Texas, at the time of his arrest.

103. An open-source query of Instagram revealed an Instagram profile under the name “Cyril LARTIGUE” utilizing the username “cyreales”. The photo associated with this account is consistent with the individual interviewed by your Affiant. This account lists 29 posts, 139 followers and 261 following. This account is set to private and no further information could be obtained.

104. An open-source query of Twitter revealed a Twitter account containing a photo consistent with LARTIGUE. In this Twitter profile: <https://twitter.com/clartigue17?lang=en>, LARTIGUE identifies himself as being from Austin, TX, and using the Twitter handle “@CLartigue17” and Twitter username “Cyril Lartigue”.

105. In LARTIGUE’s Twitter feed, on May 29, 2020 – the day before he was arrested by the Austin Police Department – LARTIGUE sent out a tweet with the caption “MAKIN’ BACON.” Attached to this tweet was a video from Dakarai Turner (@Dakari_Turner), dated May 29, 2020. Turner’s caption to the video was, “CNN just showed a video from Los Angeles of a male officer getting beat by a crowd after attempting to detain someone. What is happening around the country tonight is HISTORIC.” The attached video is of a male law enforcement

officer being attacked by protestors as he attempts to detain an individual. I know from my training and experience that “bacon” can be a derogatory reference to police.

106. LARTIGUE then retweeted a post by Jimmy Dore (@jimmy_dore), dated May 29, 2020, which read, “Cops starting violence all over the county.” In this retweet is a video showing a clash amongst law enforcement officers and protestors in San Jose, CA.

107. On May 29, 2020, LARTIGUE tweeted, “Never forget kids, all cops are bastards.”

108. LATRIGUE also retweeted a video posted by kylie (@cuddlesjk), dated May 28, 2020, which read, “I’m from hong kong and protestors here have some of the smartest tactics when fighting with our own police brutality. Here is an example of how they put out tear gas. I’ll share more if y’all need.” The post is a video of protestors placing a traffic cone over a tear gas canister and extinguishing the canister by dousing it in water. This same technique was explained to your Affiant by LARTIGUE during their interview on 06/08/2020.

109. On July 17, 2020, your Affiant obtained a federal search warrant, Case No: 1:20-mj-608-SH, issued by United States Magistrate Judge Susan Hightower allowing for the digital forensic examination of the cellular phone found amongst LARTIGUE’s possessions at the time of his arrest.

110. On July 29, 2020, your Affiant supplied the aforementioned search warrant and cellular phone to Travis County District Attorney Sergeant Investigator (SI) Manuel Fuentes for digital forensic examination. As per SI Fuentes, this phone was further identified as an Apple iPhone 11, N104P, IMEI/MEID: 352907111193009, Telephone Number: (512) 586-3046, SIM Card ICCID: 8901260232748879553. SI Fuentes was only able to obtain a partial extraction of the cellular phone. SI Fuentes was able to obtain LARTIGUE’s Apple ID:

clartigue10@gmail.com. Further digital examination revealed this email was additionally linked to the following of LARTIGUE's accounts: Gmail, Messages, Device Locator, Find My Friends, CloudKit, and iCloud.

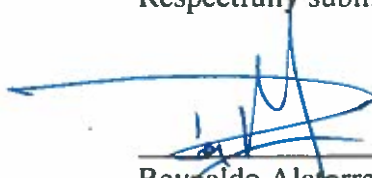
CONCLUSION

111. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations, or attempted violations, of Title 26, United States code, Section 5861(d) may be located within the above-listed **Target Accounts**.

112. Based on the forgoing, I request that the Court issued the proposed search warrants.

113. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of these warrants. The government will execute these warrants by serving them to service provider personnel, who will be directed to produce those accounts and files. Because the warrant will be served on these service providers, who will then compile the requested records at a time convenient to them, there exists reasonable cause to permit the execution of the requested warrants at any time in the day or night.

Respectfully submitted,

A handwritten signature in blue ink, appearing to be 'Reynaldo Alatorre Jr.', written over a horizontal line.

Reynaldo Alatorre Jr.
ATF Special Agent

Sworn to and subscribed to me by telephone under Rule 4.1 of the Federal Rules of Criminal Procedure on September 29, 2020.

A handwritten signature in blue ink, appearing to be 'Susan Hightower', written over a horizontal line.

SUSAN HIGHTOWER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

I. Property to Be Searched

This warrant applies to information associated with the Facebook user ID:

<https://www.facebook.com/profile.php?id=100008210433667>

that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

II. Information to be disclosed by Facebook

To the extent that the information described in this Attachment, is within the possession, custody, or control of Facebook Inc. (“Facebook”), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities **from May 23, 2020 to June 6, 2020;**
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them **from May 23, 2020 to June 6, 2020**, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;

- (d) All profile information;
- (e) **From May 23, 2020 to June 6, 2020**, all News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (f) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (g) All other records and contents of communications and messages made or received by the user **from May 23, 2020 to June 6, 2020**, including all Messenger activity, private messages, chat history, and video and voice calling history;
- (h) All "check ins" and other location information **from May 23, 2020 to June 6, 2020**;
- (i) All IP logs, including all records of the IP addresses that logged into the account;
- (j) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked" **from May 23, 2020 to June 6, 2020**;
- (k) All information about the Facebook pages that the account is or was a "fan" of;

- (l) All lists of friends created by the account **from May 23, 2020 to June 6, 2020**;
- (m) All records of Facebook searches performed by the account **from May 23, 2020 to June 6, 2020**;
- (n) The types of service utilized by the user;
- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (q) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within fourteen days of issuance of this warrant.

III. Information to be seized by the government

All information described above in Section II that constitutes fruits, evidence and instrumentalities of violations of Title 26, United States Code, 5861(d) involving Cyril Laurence Lartigue on or about May 30, 2020, including, for each user ID identified on Attachment A, Section I, information pertaining to the following matters:

- (a) Possession/Manufacture of an unregistered destructive device; and
communications with other persons, known or unknown, involved in the
aforementioned criminal activity.
- (b) Evidence indicating how and when the Facebook account was accessed or used,
to determine the chronological and geographic context of account access, use, and
events relating to the crime under investigation and to the Facebook account
owner;
- (c) Evidence indicating the Facebook account owner's state of mind as it relates to
the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records
that help reveal the whereabouts of such person(s).
- (e) The identity of person(s) who communicated with the user ID about matters
relating to the possession/manufacture of an unregistered destructive device,
including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO
FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Facebook, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Facebook. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Facebook, and they were made by Facebook as a regular practice; and

b. such records were generated by Facebook's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Facebook in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Facebook, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT B

I. Property to Be Searched

This warrant applies to information associated with the Instagram profile with username:

<https://www.instagram.com/cyreales/>

that is stored at premises owned, maintained, controlled, or operated by Instagram, LLC, a company that is owned by Facebook, Inc. and headquartered in Menlo Park, California.

II. Information to be disclosed by Instagram, LLC

To the extent that the information described in this Attachment, is within the possession, custody, or control of Instagram, LLC, including any messages, records, files, logs, or information that have been deleted but are still available to Instagram, LLC, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Instagram, LLC is required to disclose the following information to the government for each account listed in Attachment A:

- (a) All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;
- (b) All past and current usernames associated with the account;
- (c) The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
- (d) All activity logs including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information;
- (e) All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;
- (f) All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;
- (g) All communications or other messages sent or received by the account **from May 23, 2020 to June 6, 2020**;

- (h) All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content **from May 23, 2020 to June 6, 2020;**
- (i) All photographs and images in the user gallery for the account **from May 23, 2020 to June 6, 2020;**
- (j) All location data associated with the account, including geotags **from May 23, 2020 to June 6, 2020;**
- (k) All data and information that has been deleted by the user **from May 23, 2020 to June 6, 2020;**
- (l) A list of all of the people that the user follows on Instagram and all people who are following the user (*i.e.*, the user's "following" list and "followers" list), as well as any friends of the user, **from May 23, 2020 to June 6, 2020;**
- (m) All privacy and account settings;
- (n) All records of Instagram searches performed by the account, including all past searches saved by the account **from May 23, 2020 to June 6, 2020;**
- (o) All information about connections between the account and third-party websites and applications; and,
- (p) All records pertaining to communications between Instagram, LLC and any person regarding the user or the user's Instagram account, including contacts with support services, and all records of actions taken, including suspensions of the account.

Instagram is hereby ordered to disclose the above information to the government within fourteen days of issuance of this warrant.

III. Information to be seized by the government

All information described above in Section II that constitutes fruits, evidence and instrumentalities of violations of Title 26, United States Code, Section 5861(d) involving Cyril Laurence Lartigue on or about May 30, 2020, including, for each username identified on this Attachment, information pertaining to the following matters:

- (a) Possession/Manufacture of an unregistered destructive device; and
communications with other persons, known or unknown, involved in the
aforementioned criminal activity.
- (b) Evidence indicating how and when the Instagram account was accessed or used,
to determine the chronological and geographic context of account access, use, and
events relating to the crime under investigation and to the Instagram account
owner;
- (c) Evidence indicating the Instagram account owner's state of mind as it relates to
the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records
that help reveal the whereabouts of such person(s).
- (e) The identity of person(s) who communicated with the user ID about matters
relating to the possession/manufacture of an unregistered destructive device,
including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Instagram, LLC, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Instagram, LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Instagram, LLC, and they were made by Instagram, LLC as a regular practice; and

b. such records were generated by Instagram, LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Instagram, LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Instagram, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT C

I. Property to Be Searched

This warrant applies to information associated with the Twitter profile with username:

<https://twitter.com/clartigue17?lang=en>

That is stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered in San Francisco, California.

II. Information to be disclosed by Twitter

To the extent that the information described in this Attachment, is within the possession, custody, or control of Twitter, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each user ID listed in this Attachment for the period **from May 23, 2020 to June 6, 2020**:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All past and current usernames, account passwords, and names associated with the account;
- (c) The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;

- (d) All IP logs and other documents showing the IP address, date, and time of each login to the account;
- (e) All data and information associated with the profile page, including photographs, “bios”, and profile backgrounds and themes;
- (f) All “Tweets” and Direct Messages sent, received “favorited”, or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;
- (g) All photographs and images in the user gallery for the account;
- (h) All location data associated with the account, including all information collected by the “Tweet With Location” service;
- (i) All information about the account’s use of Twitter’s link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;
- (j) All data and information that has been deleted by the user;
- (k) A list of all the people that the user follows on Twitter (i.e., the user’s “following” list);
- (l) All “lists” created by the account;
- (m) All information on the “Who to Follow” list for the account;
- (n) All privacy and account settings;

- (o) All records of Twitter searches performed by the account, including all past searches saved by the account;
- (p) All information about connections between the account and third-party websites and applications;
- (q) All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

III. Information to be seized by the government

All information described above in this Attachment that constitutes fruits, evidence and instrumentalities of violations of Title 26, United States Code, 5861(d) involving Cyril Laurence Lartigue on or about May 30, 2020, including, for each user ID identified in this Attachment, information pertaining to the following matters:

- (a) Possession/Manufacture of an unregistered destructive device; and communications with other persons, known or unknown, involved in the aforementioned criminal activity.
- (b) Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime.
- (c) Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner;

- (d) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;
- (e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (f) The identity of person(s) who communicated with the user ID about matters relating to the possession/manufacture of an unregistered destructive device, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Instagram, LLC, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Instagram, LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Instagram, LLC, and they were made by Instagram, LLC as a regular practice; and

b. such records were generated by Instagram, LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Instagram, LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Instagram, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT D

I. Property to Be Searched

This warrant applies to information associated with the following electronic accounts:

Clartigue10@gmail.com

That is stored at premises owned, maintained, controlled, or operated by Google, Inc. (“Google”), a company headquartered in Mountain View, California.

II. Information to be disclosed by Google, Inc. (the “Provider”)

To the extent that the information described in this Attachment, is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in this Attachment for the period **from May 23, 2020 to June 6, 2020**:

- (a) The contents of all emails or other communications (including instant messages, Google Hangout, and other) associated with the account, including stored or preserved copies of emails/communications sent to and from the account, draft emails/communications, the source and destination addresses associated with each email/communication, the date and time at which each email/communication was sent, and the size and length of each email/communication.
- (b) The contents of any file storage associated with this account, such as Google Drive.

- (c) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number).
- (d) The types of service utilized.
- (e) All records or other information stored during the relevant time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures and files.
- (f) All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

III. Information to be seized by the government

All information described above in Section II that constitutes fruits, evidence and instrumentalities of violations of Title 26, United States Code, 5861(d) involving Cyril Laurence Lartigue on or about May 30, 2020, including, for each account or identifier listed in this Attachment, information pertaining to the following matters:

- (g) Possession/Manufacture of an unregistered destructive device; and communications with other persons, known or unknown, involved in the aforementioned criminal activity.

- (h) Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime.
- (i) Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner;
- (j) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;
- (k) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (l) The identity of person(s) who communicated with the user ID about matters relating to the possession/manufacture of an unregistered destructive device, including records that help reveal their whereabouts.
- (m) Account history (including Terms of Service and any complaints) and billing records (including date, time, duration, and screen names used each time the account was activated).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Instagram, LLC, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Instagram, LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Instagram, LLC, and they were made by Instagram, LLC as a regular practice; and

b. such records were generated by Instagram, LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Instagram, LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Instagram, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT E

I. Property to Be Searched

This warrant applies to information associated with the following Apple Inc., iCloud storage and email account

Subscriber: Cyril Laurence Lartigue

Emails: Clartigue10@gmail.com; and/or subscriber Cyril Laurence Lartigue; and/or associated with telephone number: (512) 586-3046; and/or the associated email address ending in “@icloud.com,” or “@me.com,” or “@mac.com,” which is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered in Cupertino, California.

II. Information to be disclosed by Apple Inc.

To the extent that the information described in this Attachment, is within the possession, custody, or control of Apple Inc., including any messages, records, files, logs, or information that have been deleted but are still available to Apple Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple Inc., is required to disclose the following information to the government for each account or identifier listed in this Attachment:

- a. All records or other information regarding the identification of the account, to include full name, e-mail addresses provided, physical address, telephone numbers and other identifiers, records of session times and durations, the time and date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, any other accounts linked to

this user or e-mail, and means and source of payment (including any credit or bank account number);

- b. All location information related to the account **from May 23, 2020 to June 6, 2020**, to include the mobile device location, GPS, or IP addresses associated with the account, logins, or posts;
- c. Any other Apple accounts accessed by this user;
- d. The contents of all e-mails and instant messages sent or received from **May 23, 2020 to June 6, 2020** and stored in the account, including copies of e-mails and instant messages sent to and from the account, draft e-mails and instant messages, the source and destination addresses associated with each e-mail and/or instant message, the date and time at which each e-mail or instant message was sent, and the size and length of each e-mail or instant message;
- e. The contents of all instant messages sent or received **from May 23, 2020 to June 6, 2020** and stored in the account, including copies of messages sent to and from the account, draft messages, the source and destination addresses associated with each message, the date and time at which a message was sent/received, and the size and length of each message;
- f. Any deleted e-mails or instant messages sent or received from May 23, 2020 to June 6, 2020, including any information described in subparagraphs “d” and “e” above;
- g. All photographs, messages, iOS device backups, or other content stored in the iCloud account from May 23, 2020 to June 6, 2020, and all information pertaining to the source or such photographs and other stored content;

- h. Record of all accesses of the account **from May 23, 2020 to June 6, 2020**, including the times, dates, IP addresses, device used (identifiers and type), device location data, and browser used associated with these accesses;
- i. All address books, contact and buddy lists, calendar data, pictures, and files stored **from May 23, 2020 to June 6, 2020**;
- j. All records pertaining to communications between Apple Inc. and any person regarding the account, including contacts with support services and records of action taken; and
- k. All records associated with the other services provided with an iCloud account, to include: iCloud, Groups, Office, Photographs, Spaces, iTunes and iPhones.

III. Information to be seized by the government

- 1. All records and information described in Section II above that constitutes fruits, evidence, and instrumentalities of violations of Title 26, United States Code, Section 5861(d) including, for each account and identifier listed on this Attachment, the following:
 - a. All files, including, but not limited to, communications, images, and videos related to the possession/manufacture of an unregistered destructive device;
 - b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts; and
- 2. Evidence of who used, owned, or controlled the account or identifier listed on this Attachment;
- 3. Evidence of the times the account or identifier listed on this Attachment was used;
- 4. Passwords and/or encryption keys, and other access information that may be necessary to access the account or identifier listed on this Attachment and other associated accounts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO
FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Instagram, LLC, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Instagram, LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Instagram, LLC, and they were made by Instagram, LLC as a regular practice; and
- b. such records were generated by Instagram, LLC's electronic process or system that produces an accurate result, to wit:
 1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Instagram, LLC in a manner to ensure that they are true duplicates of the original records; and
 2. the process or system is regularly verified by Instagram, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature